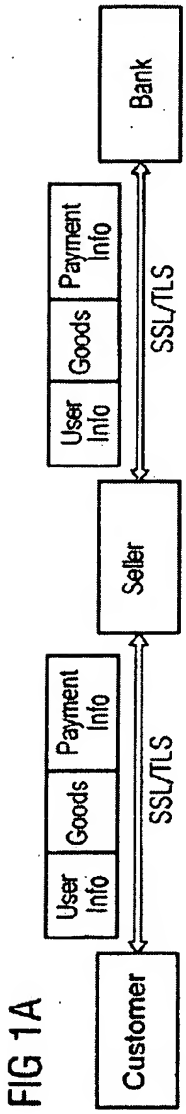

Bank
Payment Info
Goods
User Info
SSL/TLS
Seller
Payment Info
Goods
User Info
SSL/TLS
Customer

FIG 1A

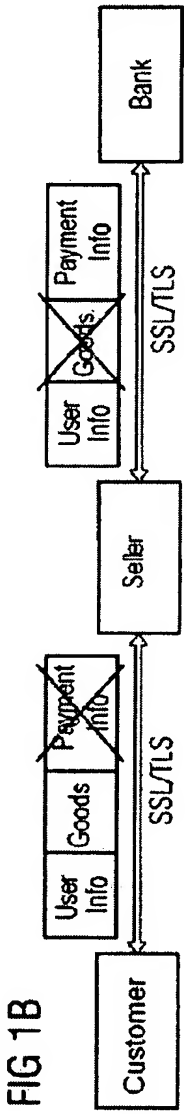

Bank
Payment Info
Goods
User Info
SSL/TLS
Seller
Payment Info
Goods
User Info
SSL/TLS
Customer

FIG 1B

FIG 2A

Attribute	Encrypted Attribute Extension
VISA	$E(K_{VISAPublicKey}, CreditCardNumber)$
American Express(AMEX)	$E(K_{AMEXPublicKey}, CreditCardNumber)$
MasterCard	$E(K_{MasterCardPublicKey}, CreditCardNumber)$
Bank Account	$E(K_{BankPublicKey}, AccountNumber)$
Address	$E(K_{PostPublicKey}, Address)$
Social Insurance Number	$E(K_{InsurancePublicKey}, InsuranceNumber)$

Table 1.1: New certificate extensions.

FIG 2B

OID	Value
1. 3. 6. 1. 4. 15601	Root node of new extensions
1. 3. 6. 1. 4. 15601. 1	Encrypted value: VISA credit card number
1. 3. 6. 1. 4. 15601. 2	Encrypted value: American Express credit card number
1. 3. 6. 1. 4. 15601. 3	Encrypted value: MasterCard credit card number
1. 3. 6. 1. 4. 15601. 4	Encrypted value: Bank account number
1. 3. 6. 1. 4. 15601. 5	Encrypted value: Address
1. 3. 6. 1. 4. 15601. 6	Encrypted value: Social insurance number

Table 1.2: New private OIDs.

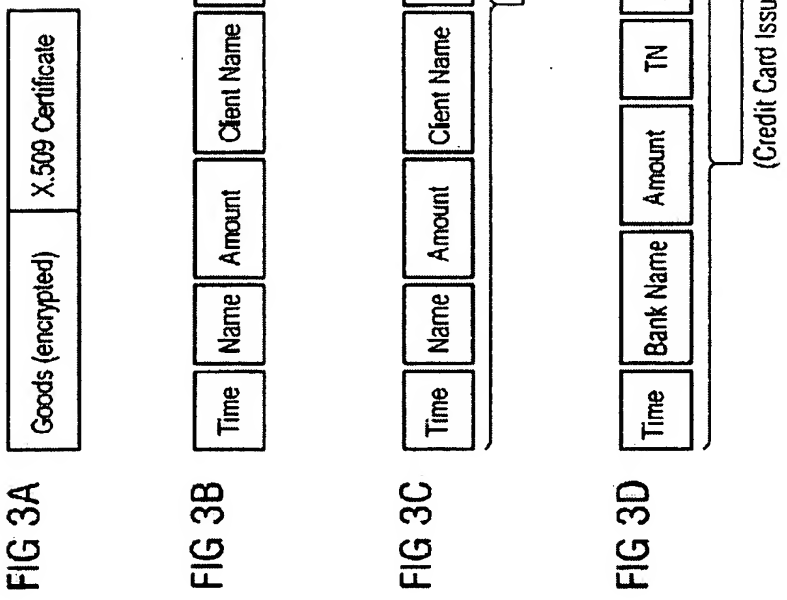


FIG 3A

FIG 3B

FIG 3C

FIG 3D

FIG 3E

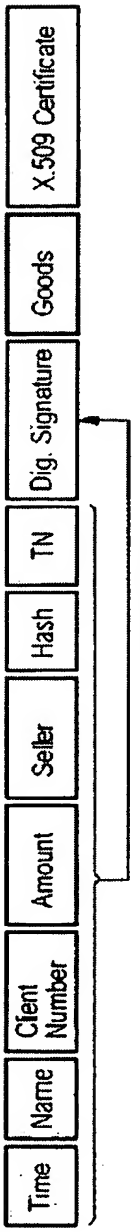


FIG 3F

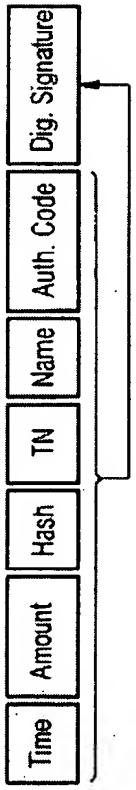


FIG 3G

User request format:

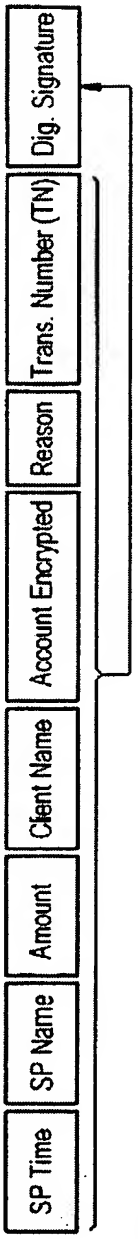


FIG 3H

Credit Card Issuer response format:

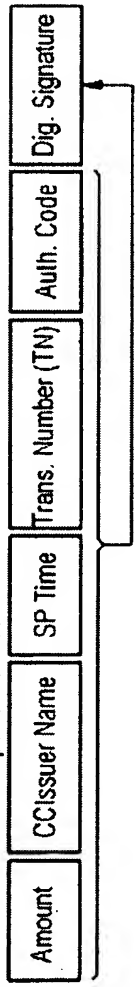


FIG 4

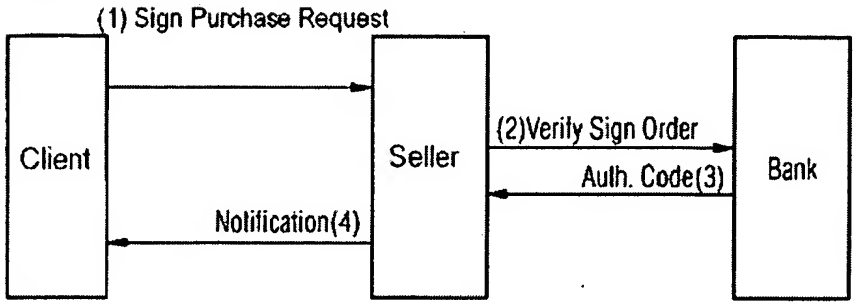

(1) Sign Purchase Request
Client
Seller
Bank
(2)Verify Sign Order
Auth. Code(3)
Notification(4)

FIG 5

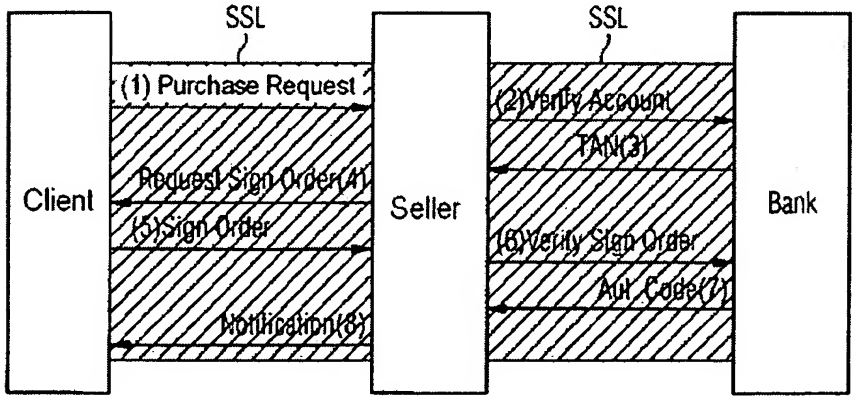
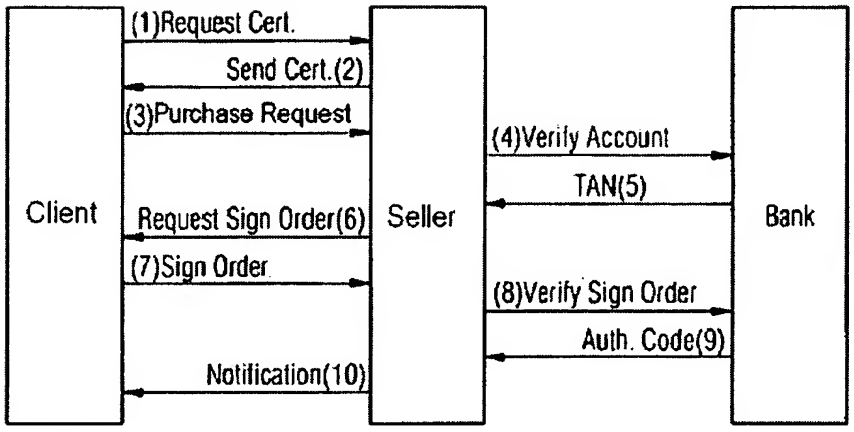

SSL
SSL
Client
Seller
Bank
(1) Purchase Request
Request Sign Order(4)
(5)Sign Order
Notification(8)
(2)Verify Account
TAN(3)
(6)Verify Sign Order
Aut. Code(7)

FIG 6


Client
Seller
Bank
(1)Request Cert.
Send Cert.(2)
(3)Purchase Request
(4)Verify Account
TAN(5)
Request Sign Order(6)
(7)Sign Order
(8)Verify Sign Order
Auth. Code(9)
Notification(10)

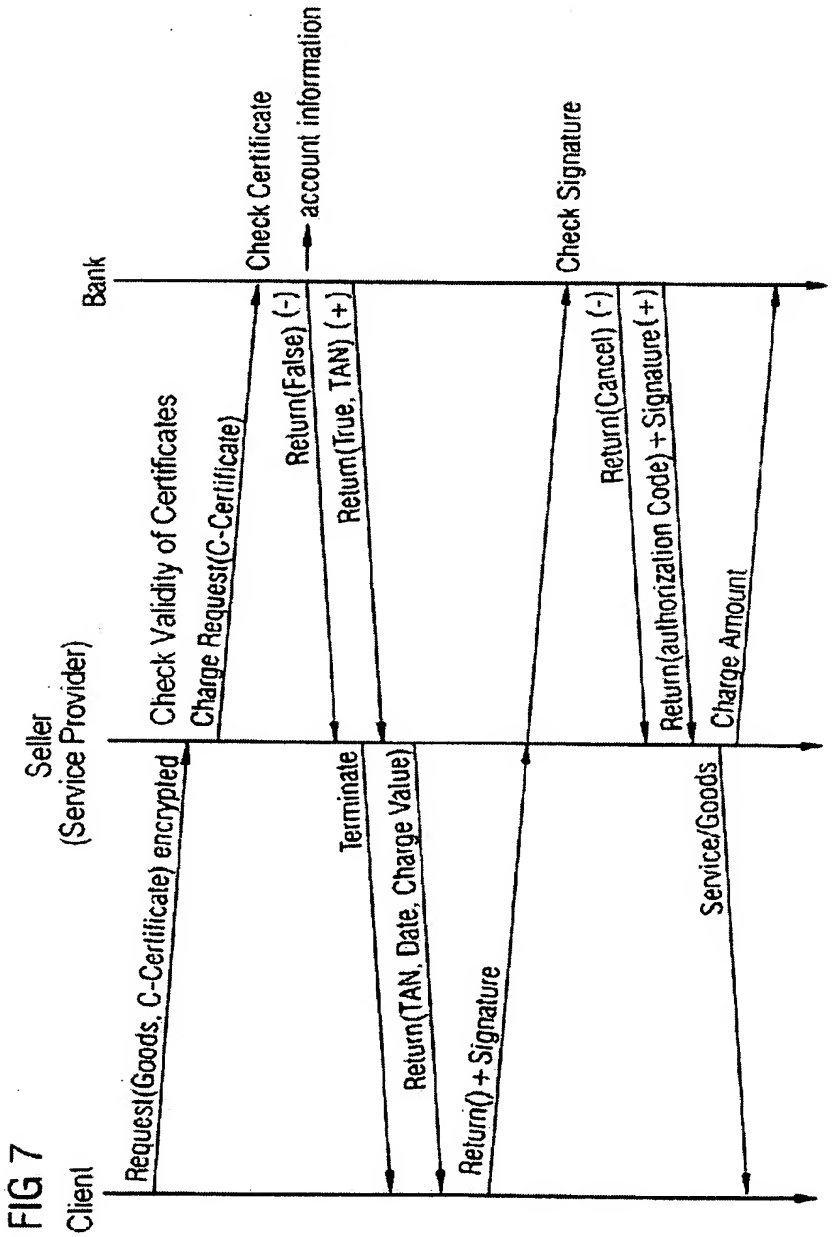

Client
Seller
(Service Provider)
Bank
Request(Goods, C-Certificate) encrypted
Check Validity of Certificates
Charge Request(C-Certificate)
Check Certificate
account information
Return(False) (-)
Return(True, TAN) (+)
Terminate
Return(TAN, Date, Charge Value)
Return() + Signature
Check Signature
Return(Cancel) (-)
Return(authorization Code) + Signature (+)
Charge Amount
Service/Goods

FIG 7

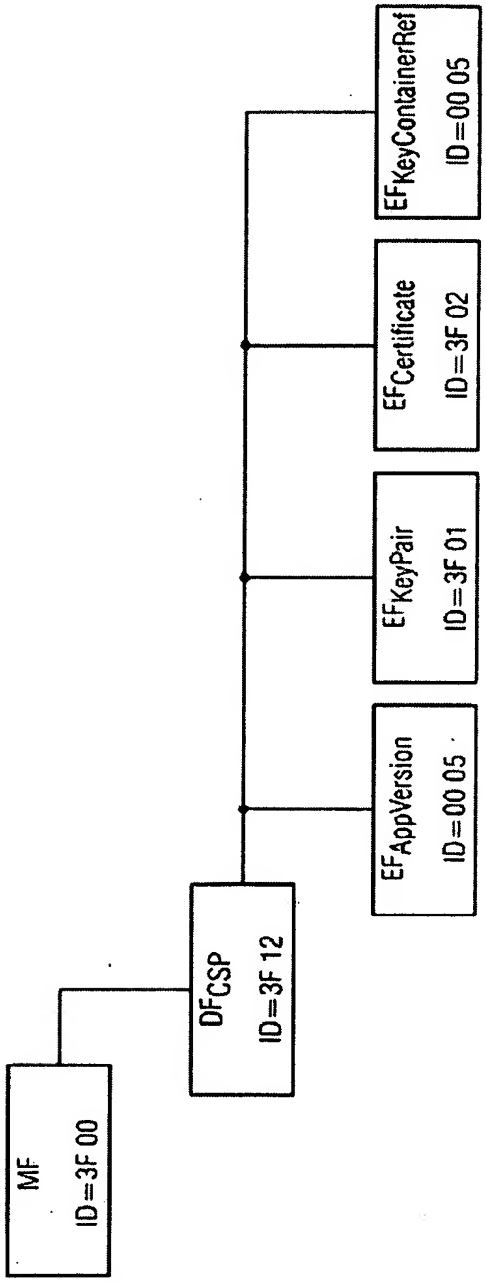

MF
ID=3F 00
DFCSP
ID=3F 12
EFAppVersion
ID=00 05
EFKeyPair
ID=3F 01
EFCertificate
ID=3F 02
EFKeyContainerRef
ID=00 05

FIG 8

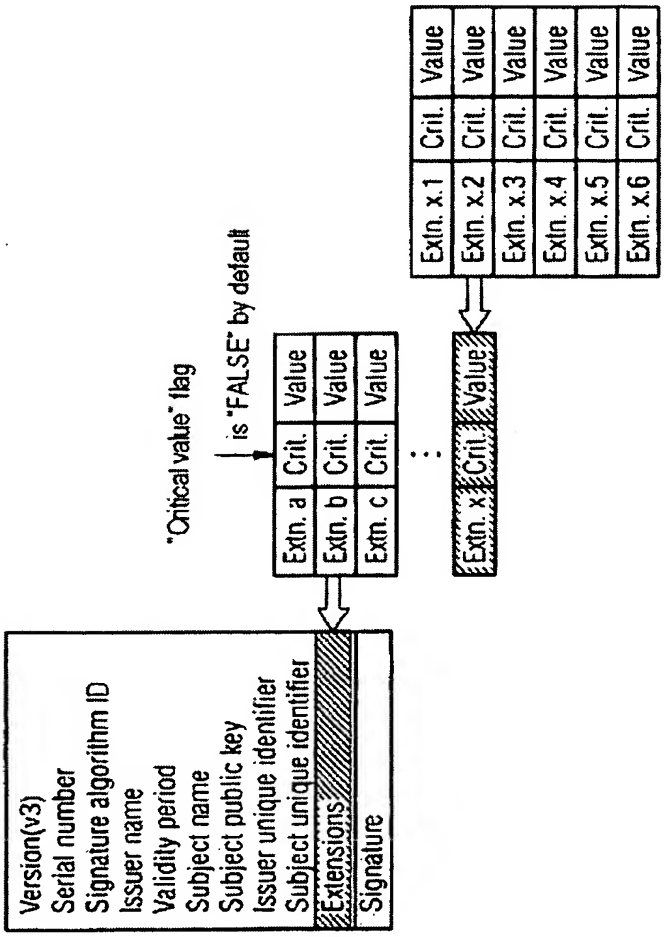

Version(v3)
Serial number
Signature algorithm ID
Issuer name
Validity period
Subject name
Subject public key
Issuer unique identifier
Subject unique identifier
Extensions
Signature
"Critical value" flag
is "FALSE" by default
Extn. a
Extn. b
Extn. c
Extn. x
Crit.
Value
Extn. x.1
Extn. x.2
Extn. x.3
Extn. x.4
Extn. x.5
Extn. x.6

FIG 9